UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,953	11/30/2000	Guy McIlroy	PALM-3281.US.P	5875

49637 7590 11/13/2008

BERRY & ASSOCIATES P.C.
9255 SUNSET BOULEVARD
SUITE 810
LOS ANGELES, CA 90069

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/727,953	MCILROY, GUY	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-2 and 4-21* is/are pending in the application.

4a) Of the above claim(s) *22-28* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 May 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Claim 3 has been cancelled. Applicant's arguments/amendments with respect to the pending claims filed 7/31/2008 have been fully considered but are moot in view of new grounds rejection. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2 and 4-21 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 8, and 18 recite the limitation "…the desired platform…" in the limitation added by the amendment. There is insufficient antecedent basis for this limitation in the claim since a desired platform was not previously introduced in the claim.

Claims not specifically addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-2, 4-5, 7-13, 15-18, and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mohammed et al., US Patent No. 6,374,357 and further in view of Brody, US Pub. No. 2001/0051928 and Muttik et al., US Patent No. 6,907,396.

As per claim 1:

Mohammed et al. teach a method of ensuring the security of a computer system, comprising loading software on said computer system suitable for operating on the computer system (col. 6, lines 12-32 and col. 18, lines 13-15); upon loading the software on the computer system, validating said software by the use of a validator program that scans the software that is loaded in a secure environment (col. 18, line 56 – col. 19, line 5); marking said software as valid or invalid by the use of a flag (col. 18, line 63 – col. 19, line 15); and, denying said software the ability to operate on any environment within said computer system if said validator fails to identify said software as valid in order to ensure the security of said computer system (col. 19, lines 4-12). Furthermore, Mohammed et al. teach that the computing environment allows for various computing systems, one of which may be a handheld device (col. 6, lines 21-26).

Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer where the software is validated by the use of a validator program, residing in the computer system in a secure fashion such that the validator programs scans the software that is loaded in a secure environment. However, Brody teaches a PDA coupled to a host device for personalization purposes. Furthermore, Brody et al. teach that one of the steps during the personalization process may be to

scan the software before allowing it to be downloaded to the PDA to prevent from downloading an application with malicious code (par. 105). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the portable device, where one of the functions includes the PDA having a validation program stored in a secure fashion in order to scan the software. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA, as well as to validate an application before downloading it to the PDA, in par. 33, lines 1-30 and par. 163.

Also not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However, Muttik et al. teach the use of an emulator to run code that has potentially been infected (col. 5, lines 13-18). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. for the validating and scanning of the software to include running the code in an emulator in order to examine the code for malicious routines. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that

running code in an emulator in order to protect the computer system from unnecessary damages to the system if the code is malicious in col. 4, lines 15-23.

As per claim 2:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the method described in claim 1. Furthermore, Mohammed et al. teach wherein said method operates on an open platform computer system (col. 5, line 66 – col. 6, line 32).

As per claim 4:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the method described in claim 1. Furthermore, Mohammed et al. teach wherein said software is supplied by a third-party source (col. 9, lines 51-63).

As per claim 5:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the method described in claim 4. Furthermore, Mohammed et al. teach wherein said third-party software is for execution or other use on a palmtop computer (col. 6, lines 33-38).

As per claim 7:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the method described in claim 1. Mohammed et al. also teach a host computer (col. 6, lines 33-38). Furthermore, Mohammed et al. teach that the computing environment allows for various computing systems, one of which may be a handheld device (col. 6, lines 21-26). Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer and wherein the validating operation is performed by the host computer for the portable computing device. However, Brody teaches a PDA coupled to a host

device for personalization purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the palmtop computing device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA in par. 33, lines 1-30.

As per claim 8:

Mohammed et al. substantially teach an apparatus for ensuring the security of software in a computer system, comprising a validation program that is capable of validating said software by first scanning said software that is loaded in a secure environment (col. 18, line 56 – col. 19, line 5); marking said software as valid or invalid by the use of a flag (col. 18, line 63 – col. 19, line 15); and, denying said software the ability to operate in any environment on said computer system if said validator program fails to identify said software as valid in order to ensure the security of said computer system (col. 19, lines 4-12). Furthermore, Mohammed et al. teach that the computing environment allows for various computing systems, one of which may be a handheld device (col. 6, lines 21-26).

Not explicitly disclosed is wherein said method operates on a computer system which comprises a portable computing device coupled to said host computer where the software is validated by the use of a validator program, residing in the computer system in a secure fashion such that the validator programs scans the software that is loaded in a secure environment.

However, Brody teaches a PDA coupled to a host device for personalization purposes. Furthermore, Brody et al. teach that one of the steps during the personalization process may be to scan the software before allowing it to be downloaded to the PDA to prevent from downloading an application with malicious code (par. 105). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the portable device, where one of the functions includes the PDA having a validation program stored in a secure fashion in order to scan the software. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA, as well as to validate an application before downloading it to the PDA, in par. 33, lines 1-30 and par. 163.

Also not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However, Muttik et al. teach the use of an emulator to run code that has potentially been infected (col. 5, lines 13-18). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. for the validating and scanning of the software to include running the code in an emulator in order to examine the code for malicious routines. This modification would have been obvious because a person having ordinary skill in the art, at the

time the invention was made, would have been motivated to do so since Muttik et al. suggest that running code in an emulator in order to protect the computer system from unnecessary damages to the system if the code is malicious in col. 4, lines 15-23.

As per claim 9:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Brody teaches wherein said host computer is coupled to a network (par. 33, lines 1-30).

As per claim 10:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Brody teaches wherein said portable computing device is a handheld computing device (par. 33, lines 1-30).

As per claim 11:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Brody teaches wherein said portable computing device is a personal data assistant (par. 33, lines 1-30).

As per claim 12:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Brody teaches wherein said portable computing device is coupled to said host computer by an infrared device (par. 33, lines 25-30).

As per claim 13:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Furthermore, Brody teaches wherein said portable computing device is coupled to said host computer by an RF enabled device (par. 33, lines 25-30).

As per claim 15:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Mohammed et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software if said third-party software is not found to be clean of known security compromising routines (col. 18, line 35 – col. 19, line15).

As per claim 16:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 15. Mohammed et al. further teach wherein said portable computing device is configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached (col. 19, lines 4-15).

As per claim 17:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described claim 15. Furthermore, Brody teaches wherein said portable computing device is a personal data assistant (par. 33, lines 1-30).

As per claim 18:

Mohammed et al. substantially teach an apparatus for ensuring the security of a computer system, comprising a validation program that is capable of validating said software by scanning the files of said software in a secure environment on the handheld computing device upon loading the software in any environment on the handheld computing device (col. 18, line 56 – col. 19, line 5); marking said software as valid or invalid by the use of a flag (col. 18, line 63 – col. 19, line 15); and denying said software the ability to operate on any environment on said computer system if said validator fails to identify said software as valid in order to ensure the security of said computer system (col. 19, lines 4-12). Furthermore, Mohammed et al. teach that the computing environment allows for various computing systems, one of which may be a handheld device (col. 6, lines 21-26).

Not explicitly disclosed is wherein a handheld computing device couple to a network, wherein said handheld computing device is capable of loading software from said network to said handheld computing device for operating on said handheld computing device where the validation program resides on a network such that the validation program scans the software that is loaded in a secure environment before it is loaded onto the handheld computing device. However, Brody teaches a PDA coupled to a host computer (which is in a secure networked environment) for personalization purposes. Furthermore, Brody et al. teach that one of the steps during the personalization process may be to scan the software before allowing it to be downloaded to the PDA to prevent from downloading an application with malicious code (par. 105). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. to have the hand-held device coupled to the host computer in order to carry out different functions on the portable device, where one of

the functions includes the PDA having a validation program stored in a secure fashion in order to scan the software. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Brody suggests that PDA's are used in conjunction with PC's in order to download applications because PDA's are highly mobile and the client can always have access to his/her PDA, as well as to validate an application before downloading it to the PDA, in par. 33, lines 1-30 and par. 163.

Also not explicitly disclosed is wherein the act of scanning and validating comprises running the code in an emulator for the desired platform within the secure environment for the emulator to run in, allowing the execution of the code to be examined for any new malicious routines as well as against known malicious signatures. However, Muttik et al. teach the use of an emulator to run code that has potentially been infected (col. 5, lines 13-18). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. for the validating and scanning of the software to include running the code in an emulator in order to examine the code for malicious routines. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Muttik et al. suggest that running code in an emulator in order to protect the computer system from unnecessary damages to the system if the code is malicious in col. 4, lines 15-23.

As per claim 20:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 18. Mohammed et al. further teach wherein said portable computing device is

configured to load third-party software files with said digital "valid" flag attached and to refrain from loading third-party software files which have no flag attached or have said "invalid" flag attached (col. 19, lines 4-15).

As per claim 21:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 18. Mohammed et al. further teach wherein said validation program is configured to evaluate third-party software and attach a digital "valid" flag if said third-party software is found to be clean of known security compromising routines or attach a digital "invalid" flag to said third-party software if said third-party software is not found to be clean of known security compromising routines (col. 18, line 35 – col. 19, line15).

III. Claims 6, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mohammed et al., US Patent No. 6,374,357; Brody, US Pub. No. 2001/0051928; and Muttik et al., US Patent No. 6,907,396 as applied to claims 1, 8, & 18 above, and further in view of Ginter et al., US Patent No. 6,948,070.

As per claim 6:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the method described in claim 1. Not explicitly disclosed is wherein said validator program is specially constructed to reside in a secure fashion in the host facility of said computer system. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Mohammed et al. for the validator program to be contained

within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 14:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 8. Not explicitly disclosed is wherein said validation program resides in said host computer of the computer system in a fashion intended to be secure. However, Ginter et al. teach the use of a tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Mohammed et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

As per claim 19:

Mohammed et al., Brody et al. and Muttik et al. substantially teach the apparatus described in claim 18. Not explicitly disclosed is wherein said validation program resides in said computer network in a fashion intended to be secure. However, Ginter et al. teach the use of a

tamper-resistant security barrier which could be included in any component in a network so that processes are ensured to be carried out within a secure environment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the apparatus disclosed in Mohammed et al. for the validator program to be contained within a secure environment in order to ensure that it has not been tampered with so that it correctly validates the software/application. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Ginter et al. suggest that it is important to ensure that processes are carried out within a secure environment in col. 59, lines 48-59.

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,694,436
2. US Patent No. 5,953,502
3. US Patent No. 7,080,407

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
11/9/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437